ARIN Support for DNSSEC and RPKI

ION San Diego
11 December 2012

Pete Toscano, ARIN
DNS and BGP

- They have been around for a long time.
  - DNS: 1982
  - BGP: 1989
- They are not very secure.
- Methods for securing them exist.
DNSSEC

• Domain Name System Security Extensions

• Took a while to implement --
  • Design work started in 1993 at IETF 28.
  • The root zone signed: July 15th, 2010.
DNSSEC

• Designed to verify data integrity and authenticity.
• Does not prevent data snooping.
• Generally, that first point outweighs these others.
DNSSEC

- DNSSEC is an overlay on top of DNS, not a replacement.
- Uses public key cryptography and a chain of trust similar to X.509 certificates.
DNSSEC

• Adds six new RR types and extension mechanisms for DNS (EDNS).
  • DNSKEY
  • DS
  • RRSIG
  • NSEC
  • NSEC3
  • NSEC3PARAM
DNSSEC

- DNSKEY: The public keys. Either a Key Signing Key (KSK) or Zone Signing Key (ZSK).
- DS: Delegation Signer. Hashes and identifies the KSK of a signed, delegated child zone.
DNSSEC

- **RRSIG**: Resource Record Signature. Every RRset for each name has a single RRSIG. There are two exceptions:
  - NS records at delegation points.
  - Glue records.
- DNSKEY RRSIGs are signed by the KSK, all others by ZSK.
DNSSEC

- NSEC/NSEC3: Next Secure Record / Next Secure Record version 3.
  - Used to prove the non-existence of a resource record.
DNSSEC

• A simple example of securing a zone.

```plaintext
example.com.
  SOA [SOA STUFF]
  NS ns
  MX 10 mail

mail
  A 128.66.0.100
  AAAA 2001:db8::100

ns
  A 128.66.0.10
  AAAA 2001:db8::10

sub
  NS ns.sub

ns.sub
  A 128.66.10.10
  AAAA 2001:db8:10::10
```
DNSSEC

• Throw in the keys...

  example.com. SOA [SOA STUFF]
  NS ns
  MX 10 mail
  \[DNSKEY 256 [DNSKEY STUFF]; ZSK
  DNSKEY 257 [DNSKEY STUFF]; KSK

  mail A 128.66.0.100
  AAAA 2001:db8::100
  ns A 128.66.0.10
  AAAA 2001:db8::10
  sub NS ns.sub
  ns.sub A 128.66.10.10
  AAAA 2001:db8:10::10
DNSSEC

- Add the NSEC records so that all gaps are accounted for...

  example.com.          SOA [SOA STUFF]
  example.com.          NS  ns
  example.com.          MX  10  mail
  example.com.          DNSKEY 256 [DNSKEY STUFF]; ZSK
  example.com.          DNSKEY 257 [DNSKEY STUFF]; KSK
  example.com.          NSEC mail.example.com. SOA NS MX DNSKEY NSEC
  mail.example.com.     A   128.66.0.100
  mail.example.com.     AAAA 2001:db8::100
  mail.example.com.     NSEC ns.example.com. A AAAA NSEC
  ns.example.com.       A   128.66.0.10
  ns.example.com.       AAAA 2001:db8::10
  ns.example.com.       NSEC sub.example.com. A AAAA NSEC
  sub.example.com.      NS  ns.sub
  sub.example.com.      NSEC example.com. NS NSEC
  ns.sub.example.com.   A   128.66.10.10
  ns.sub.example.com.   AAAA 2001:db8:10::10

- NSEC doesn’t do glue.
- Zone enumeration? That’s where NSEC3 comes in.
• Sign each label’s RRset and update NSECs...

```
example.com.             SOA [SOA STUFF]
examp...
• Signed delegations. Add DS records and update NSEC and RRSIGs.

  example.com.         SOA [SOA STUFF]
  example.com.         RRSIG SOA [RRSIG STUFF]
  example.com.         NS ns
  example.com.         RRSIG NS [RRSIG STUFF]
  example.com.         MX 10 mail
  example.com.         RRSIG MX [RRSIG STUFF]
  example.com.         DNSKEY 256 [DNSKEY STUFF]; ZSK
  example.com.         DNSKEY 257 [DNSKEY STUFF]; KSK
  example.com.         RRSIG DNSKEY [RRSIG STUFF]
  example.com.         NSEC mail.example.com. SOA NS MX DNSKEY NSEC RRSIG
  example.com.         RRSIG NSEC [RRSIG STUFF]
  mail.example.com.    A 128.66.0.100
  mail.example.com.    RRSIG A [RRSIG STUFF]
  mail.example.com.    AAAA 2001:db8::100
  mail.example.com.    RRSIG AAAA [RRSIG STUFF]
  mail.example.com.    NSEC ns.example.com. A AAAA NSEC RRSIG
  mail.example.com.    RRSIG NSEC [RRSIG STUFF]
  ns.example.com.      A 128.66.0.10
  ns.example.com.      RRSIG A [RRSIG STUFF]
  ns.example.com.      AAAA 2001:db8::10
  ns.example.com.      RRSIG AAAA [RRSIG STUFF]
  ns.example.com.      NSEC sub.example.com. A AAAA NSEC RRSIG
  ns.example.com.      RRSIG NSEC [RRSIG STUFF]
  sub.example.com.     NS ns.sub
  sub.example.com.     DS [Hash of sub's KSK]
  sub.example.com.     RRSIG DS [RRSIG STUFF]
  sub.example.com.     NSEC example.com. NS DS NSEC RRSIG
  sub.example.com.     RRSIG NSEC [RRSIG STUFF]
  ns.sub.example.com.  A 128.66.10.10
  ns.sub.example.com.  AAAA 2001:db8:10::10
What to do with all this extra data?
Publishing the signed data is only half the battle.
The authoritative DNS responses need to be validated.
DNSSEC

- Response validation involves following a chain of trust from the trust anchor to the answer received.
- Typically, the root zone’s KSK == Trust Anchor
The backbone of the chain of trust is the DS, DNSKEY, RRSIG interaction.

Trust travels from the parent zone down to the child zone. Repeat until the target zone is found.

Start at the trust anchor’s zone.
DNSSEC

Parent Zone

RRSIG

KSK DNSKEY

ZSK DNSKEY

Parent Zone

RRSIG

KSK DNSKEY

ZSK DNSKEY

Child Zone

RRSIG

KSK DNSKEY

ZSK DNSKEY

Child Zone

RRSIG

DS

RRSIG

RSIG

DS
DNSSEC

- Once the target child zone is found, the ZSK is used to verify the appropriate RRSIG.
- If the question cannot be answered, the ZSK can be used to verify the appropriate NSEC/NSEC3 RRSIG.
- If the answer can’t be verified, then NXDOMAIN status is returned.
DNSSEC

- From a DNS publisher’s point of view, DNSSEC can greatly expand the size of zones.
- On average, responses are larger.
- Management of the keys can be tricky.
- Protects the data, not the headers.
- Does nothing to protect the stub resolver to recursive resolver communication.
DNSSEC

• At ARIN, we currently sign our v4 /8s and v6 /12 and /24s.
• ARIN Online allows members to add DS records to the zones their resources are delegated from.
DNSSEC

- DNSSEC Analyzer:  
  http://dnssec-analyzer.verisignlabs.com
- DNSViz:  http://dnsviz.net
- ldns / Drill:  
  http://www.nlnetlabs.nl/projects/ldns/
- DNSSEC Validator:  
  http://www.dnssec-validator.cz/ (FF Plugin)
- Other Tools:  
RPKI
“The inter-domain routing protocol BGP was created when the Internet environment had not yet reached the present, contentious state. Consequently, the BGP design did not include protections against deliberate or accidental errors that could cause disruptions of routing behavior.”

• Intro to RFC 4272 “BGP Security Vulnerabilities Analysis” January 2006
RPKI

This is the basic problem...

Send a packet to 209.85.128.100

I have 209.85.128.0/17
RPKI

165.135.0.2

AS100  

AS200  

AS300

AS666  

209.85.128.100

209.85.128.100
### RPKI

- April 1997 – AS 7007 announced paths for all of the internet to themselves.
- Feb. 24, 2008 – Pakistan Telecom announced a part of YouTube’s address blocks.
- April 2010 - China Telecom mis-originated about 15% of Internet address blocks affecting I-root.
- Nov. 2012 – Google was unavailable some places via route leak from Moratel.
RPKI

Phase 1: Origin Validation
(requires RPKI)

Phase 2: Path Validation
(still in draft phase)

165.135.0.2  AS100  AS200  AS300  209.85.128.100
RPKI

- Resource Public Key Infrastructure
- RPKI attaches ASNs and IP address blocks to X.509 v3 certs.
- These resource certs are signed by the resource parent.
RPKI

Resource Allocation Hierarchy

IANA

AFRINIC  APNIC  ARIN  LACNIC  RIPE NCC

ISP 1  ISP 2  ISP 4

ISP 3  ISP  ISP  ISP
RPKI

Certificates issued to match allocations.

Issuer: ARIN
Subject: ARIN
Resources: 192.0.0.0/8
Key Info: <arin-key-pub>
Signed: <arin-key-priv>
RPKI

Certificates issued to match allocations.

Issuer: ARIN
Subject: ISP1
Resources: 192.2.0.0/16
Key Info: <isp1-key-pub>
Signed: <arin-key-priv>

Issuer: ARIN
Subject: ARIN
Resources: 192.0.0.0/8
Key Info: <arin-key-pub>
Signed: <arin-key-priv>
RPKI

• Address holders issue Route Origin Authorizations (ROAs).
RPKI

Certificates issued to match allocations.

Issuer: ARIN
Subject: ISP1
Resources: 192.2.0.0/16
Key Info: <isp1-key-pub>
Signed: <arin-key-priv>

Issuer: ISP1
Subject: ISP3
Resources: 192.2.200.0/24
Key Info: <isp3-key-pub>
Signed: <isp1-key-priv>

Issuer: ARIN
Subject: ARIN
Resources: 192.0.0.0/8
Key Info: <arin-key-pub>
Signed: <arin-key-priv>
Certificates issued to match allocations.

ROA: “ISP 3 permits ASN 123 to originate its 192.2.200.0/24 network space.”
Two RPKI implementation types:

- Delegated: Each participating node becomes a CA and runs their own RPKI repository, delegated to by the parent CA.
- Hosted: The RIR runs the CA functionality for interested participants.
• For most participants, running a CA would be an insurmountable obstacle to the implementation of RPKI.
• This is why the hosted option exists.
RPKI

- Regardless of the method used, the RPKI repositories are published.
- TAL: Trust Anchor Locator
  - Points to the rsync entry point of that repo.
  - Includes that repo’s public key.
RPKI

- Reliant third parties would gather all relevant TALs.
- Get all of the RPKI repos.
- Validate, validate, validate.
• Once we have validated ROAs and the backing resource hierarchy, what do we do?
Once we have validated ROAs and the backing resource hierarchy, what do we do?

Use ROAs to weight BGP path announcements as they’re received.
RPKI
RPKI

165.135.0.2  AS100  AS200  AS300  209.85.128.100
“Only AS 300 can originate 209.85.128.0/24 network space.”
“Only AS 300 can originate my 209.85.128.0/24 network space.”
“Only AS 300 can originate my 209.85.128.0/24 network space.”
**RPKI**

- Border routers use the RPKI with the RPKI/Router protocol.
- Implemented on Cisco IOS and Quagga. JunOS recently added.
Offload validation and origin evaluation to some other box.

“Valid”, “Invalid”, “Unknown”

What’s done with these values is up to the local policy.
RPKI

• As with DNSSEC, the more buy in, the better the security.
• Be a good netizen: certify your resources.
• Even better: publish ROAs.
• Be the best happy shiny: validate route origins as support allows.
RPKI @ ARIN

- Only hosted model is currently implemented.
- The delegated model will be released in the not-too-distant future.
- Non-repudiation requirement.
- Third parties need to sign a RPA before getting the TAL.
Future of RPKI

• Single TAL.
• Inter-RIR transfers.
• Integrated with a path validation system.
Questions